DEVELOPMENT OF IMAGE CRYPTOGRAPHIC FRAMEWORK FOR CLOUD-ENABLED ENVIRONMENT USING OPTIMIZATION ALGORITHMS

A SYNOPSIS

Submitted by

S.SHEELA
(Reg. No. 201906235)

in partial fulfilment for the award of the degree

of

DOCTOR OF PHILOSOPHY

DEPARTMENT OF COMPUTER APPLICATIONS

KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION

(DEEMED TO BE UNIVERSITY)

ANAND NAGAR, KRISHNANKOIL – 626 126

TAMIL NADU, INDIA

DECEMBER 2024

1. INTRODUCTION

Cloud computing has ushered in a new era of efficiency, scalability, and flexibility in IT infrastructure and services. Built on key technologies like virtualization, distributed computing, and networking, cloud computing abstracts physical hardware into virtual instances, allowing for dynamic resource allocation. Virtualization enhances the utilization of computing resources, while distributed computing improves fault tolerance and scalability by distributing tasks across networked servers. Networking enables seamless communication between different components within cloud architecture. Enterprises have several cloud deployment strategies to choose from, including public clouds (e.g., Google Cloud, AWS, Azure), private clouds offering more control and security, and hybrid clouds, which combine both public and private elements. Cloud computing offers notable advantages such as scalability, cost savings through pay-as-you-go models, agility, and remote accessibility. However, businesses must also address challenges related to security and regulatory compliance when adopting cloud services.

1.1 Cloud-enabled big data and its components

Cloud-enabled big data transforms how businesses handle massive amounts of data by leveraging the scalability and flexibility of cloud computing. Cloud service providers like AWS, Azure, and GCP offer scalable resources that allow businesses to manage fluctuating workloads without significant upfront investments. Cloud storage services like Amazon S3 and Google Cloud Storage ensure robust, redundant, and accessible data storage across regions, supporting various data types. Cloud-based processing frameworks like Apache Hadoop and Apache Spark enable distributed computing, allowing large datasets to be processed efficiently in parallel. Real-time streaming tools such as AWS Kinesis and Apache Kafka handle continuous data ingestion, while cloud-based data warehousing systems like Amazon Redshift and Google BigQuery provide fast querying capabilities for structured data. Additionally, cloud platforms offer

machine learning and analytics services, promoting data-driven insights that improve decision-making and foster innovation. Businesses create interactive visualizations with tools like Tableau and Power BI, while strong security measures, including encryption and compliance features, ensure data protection. Cost-effectiveness, security, and compliance are vital considerations, making cloud-enabled big data a game changer in modern data management and analytics.

1.2 Technological components of cloud-enabled big data

Cloud-enabled big data involves a complex web of technologies that allow for the efficient management and analysis of vast datasets. At the core of this system is cloud computing, which provides scalable infrastructure on demand. Key components include storage systems such as Amazon S3, Google Cloud Storage, and Azure Blob Storage, which manage massive amounts of both structured and unstructured data. These systems employ distributed architectures, using techniques like sharding and replication to ensure data reliability and accessibility.

Data flows in big data systems typically begin with large-scale data collection from multiple sources. This data is then stored in a secure environment and undergoes ETL (Extract, Transform, Load) processes to cleanse and prepare it for analysis. Distributed computing frameworks, such as Apache Hadoop and Apache Spark, enable the parallel processing of large datasets by breaking tasks into smaller units executed across multiple machines. This process is scalable thanks to the elasticity of cloud resources, which adjusts dynamically based on workload demands.

Beyond storage and processing, big data systems also rely on real-time data streaming and orchestration tools like Apache Kafka and Apache Airflow to manage workflows and ensure seamless data integration with analytics platforms. Cloud services such as Google Cloud Dataproc, Amazon EMR, and

Azure HDInsight further enhance the analysis by providing environments for machine learning and advanced analytics at scale.

Security and governance are vital in cloud-based big data systems. Measures such as encryption, access controls, and data governance frameworks ensure that sensitive information is protected and handled in compliance with regulations. Finally, Infrastructure as a Service (IaaS) forms the backbone of cloud-enabled big data systems, providing the flexibility to scale resources both horizontally (adding more machines) and vertically (upgrading existing machines) based on business needs. This allows organizations to balance performance, cost, and compliance in their big data ecosystems.

1.3 Secure data sharing protocols

In secure data-sharing environments, multiple advanced cryptographic protocols ensure the confidentiality, integrity, and trustworthiness of shared data. Techniques like Secure Multi-Party Computation (SMPC) allow multiple parties to collaboratively compute functions without exposing their private inputs. SSL/TLS protocols encrypt data during transmission, while Zero-Knowledge Proofs (ZKPs) let a party prove knowledge of a secret without revealing it. Attribute-Based Encryption (ABE) further controls access by encrypting data based on specific attributes. Blockchain-based data-sharing protocols decentralize the storage and exchange of data, ensuring its immutability and integrity. Combined with smart contracts, these technologies automate secure, trustless data exchanges. Despite some challenges, such as scalability and privacy concerns, blockchain and other cryptographic methods significantly improve secure data sharing in distributed systems, ensuring data is safely accessible while maintaining confidentiality and preventing unauthorized access.

1.4 Image encryption in cloud computing

In cloud computing, image encryption is critical for safeguarding sensitive visual data during storage and transmission. Symmetric encryption, such as AES,

ensures data confidentiality by using a single key for both encryption and decryption, offering efficiency when encrypting large image files. However, key management is a crucial challenge, necessitating secure distribution and storage solutions like key vaults and rotation systems. Alongside symmetric encryption, blockchain-based tamper-resistant storage enhances data integrity, and protocols like SSL/TLS secure data transfer. Technologies like federated learning also enable collaborative model training without sharing raw images. As encryption techniques evolve, they continue to strengthen image security in cloud environments, ensuring privacy and trust in networked settings.

1.5 Cloud service models

Cloud computing has revolutionized digital services by introducing several models that cater to diverse needs, offering varying degrees of control and management over IT resources. These models—Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)—provide scalable solutions tailored to different user requirements. SaaS delivers pre-configured applications accessible via the internet without the need for local installation or maintenance, enhancing convenience and reducing costs. PaaS offers developers an environment for building and deploying applications without managing underlying infrastructure, promoting faster innovation. IaaS provides virtualized resources such as servers and storage, granting users maximum flexibility and control over their computing environment, although it demands more technical expertise. By choosing the right model, organizations can optimize IT resources, drive innovation, and stay competitive in the digital economy.

1.6 Cloud attack

Cloud attacks are a growing concern as organizations increasingly rely on cloud infrastructure for data storage, hosting, and processing. These threats come in various forms, including phishing, malware, data breaches, and more advanced tactics like Distributed Denial-of-Service (DDoS) and side-channel

attacks. One key issue is the shared responsibility model, where cloud providers secure the infrastructure while customers are responsible for their data and applications. Incorrect security configurations or weak encryption can make organizations vulnerable. Attacks like DDoS disrupt services by overwhelming them with traffic, while side-channel and malware injection attacks exploit vulnerabilities to extract sensitive information or insert malicious code. Effective mitigation strategies, including robust encryption, secure coding practices, and resource isolation, are critical to protect cloud environments.

1.7 Security access and control mechanism

Ensuring the confidentiality, integrity, and availability of data in cloud computing relies on implementing security access and control methods, including encryption, authentication, and authorization. Authentication methods like passwords, biometrics, or multi-factor authentication verify user identities, while authorization controls define what actions users can perform based on their assigned roles. Encryption secures data both in transit and at rest, preventing unauthorized access. Access control models such as Mandatory Access Control (MAC), Role-Based Access Control (RBAC), and Discretionary Access Control (DAC) provide different ways to manage permissions. MAC enforces strict, hierarchical access based on security levels, RBAC assigns permissions based on roles within an organization, and DAC allows resource owners to control who can access their resources, offering flexibility but with potential security risks. These systems work together to protect cloud environments from unauthorized access and data breaches.

1.8 Security management in cloud computing

Cloud computing security management is a multifaceted challenge that requires a comprehensive methodology to effectively protect cloud infrastructures against a variety of threats. This approach must integrate robust security controls, including encryption, access control, intrusion detection systems, and vulnerability management, alongside a proactive risk assessment

process to identify and mitigate weaknesses. Adherence to industry standards and legal regulations, such as GDPR and HIPAA, is essential for ensuring compliance and safeguarding data privacy. Moreover, Identity and Access Management (IAM) plays a crucial role in managing user identities, ensuring least privilege access, and protecting sensitive resources. Continuous monitoring and incident response are also vital, allowing early detection and swift response to security breaches. Governance structures ensure that security management aligns with organizational objectives, promoting a culture of security awareness. With cloud environments constantly evolving, proactive threat management is key to addressing risks such as malware, ransomware, data breaches, and insider threats. Measures such as regular audits, penetration testing, and employee training help maintain the integrity, confidentiality, and availability of cloud resources. As cloud-centric attacks evolve, hybrid cloud settings must also be fortified to defend against new, emerging threats.

1.9 Traditional Methods for Enhancing Security in Cloud Computing

Conventional techniques for improving cloud computing security focus on ensuring data availability, confidentiality, and integrity through well-established methods such as encryption, network security, and access control. These techniques include firewalls, VPNs, and Intrusion Detection and Prevention Systems (IDPS) to guard networks, while encryption methods like AES, RSA, and ECC protect data in transit and at rest. Access control technologies, such as Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC), help prevent unauthorized access, and compliance with regulations like GDPR and HIPAA ensures accountability. By combining these security approaches, organizations can build a strong defence posture to safeguard cloud environments from cyber threats, unauthorized access, and data breaches.

1.10 Need for Enhancing Security in Cloud Computing

Improving cloud computing security is vital for reducing risks, protecting sensitive data, ensuring legal compliance, and maintaining the trust of stakeholders and customers. Since cloud data is processed and stored on external

servers, it raises concerns about data breaches, unauthorized access, and loss. The shared responsibility model in cloud computing mandates that both cloud providers and users fulfil their security roles to mitigate risks effectively. Implementing strong authentication, Role-Based Access Controls (RBAC), and least privilege principles helps prevent unauthorized access and insider threats. Regular monitoring of cloud environments for threats allows early detection and rapid response to incidents. Businesses must also assess the security practices of Cloud Service Providers (CSPs) through due diligence, audits, and contractual agreements to ensure they meet industry standards.

1.11 Challenges for Enhancing Security in Cloud Computing

The dynamic nature of cloud environments, shared responsibility models, and emerging threats pose significant challenges to enhancing cloud computing security. One key issue is maintaining data privacy in a shared environment while complying with laws such as GDPR, HIPAA, or PCI DSS, which necessitates the use of encryption, access controls, and data residency requirements. Protecting cloud networks from threats like DDoS attacks, network sniffing, and man-in-the-middle attacks requires firewalls, IDS/IPS systems, and network segmentation. Incident response strategies must be developed and tested to swiftly detect, contain, and resolve security breaches, with forensic investigations determining the root causes. To minimize human error, staff and users should be trained in security best practices, such as strong password policies, phishing awareness, and social engineering prevention. Finally, protecting data in transit and at rest through methods like data masking, tokenization, and encryption is critical to reducing the risks associated with exposed data.

1.12 Main Contribution of The Thesis

The main contributions of the thesis are as follows,

- For secure transmission in cloud computing, the declared MFO-CBIE approach combines mayfly optimization with chaos-based image

encryption. It consists of three steps: encrypting the image with CBIE, generating the best keys possible with MFO, and decrypting the image once the cypher is accessed from the cloud server.

- The creation of the ABOA-QKIE methodology, which combines the artificial butterfly optimization algorithm with quantum key encryption for cloud security. This approach guarantees secure image encryption while simultaneously improving overall security in cloud environments by optimizing the key generation process.

- To prevent data theft in cloud computing, an ideal user authentication mechanism is created. Additionally, the jellyfish optimization algorithm is included for improved safe data storage. This approach, which was extensively tested, exhibits better performance metrics than other approaches such as RSA and ECC-based cryptography

- Enhanced cryptographic framework that utilizes the Improved Honey Badger Algorithm (HBA) to facilitate efficient data storage and robust encryption and decryption of images. The Improved HBA, known for its superior optimization capabilities, is integrated into the encryption process to generate highly secure keys and optimize the encryption mechanism. a novel multi-factor authentication (MFA) protocol that combines biometric verification and one-time password (OTP) generation is introduced. This protocol ensures robust user authentication and prevents unauthorized access.

2. LITERATURE REVIEW

2.1 Review on Security Enhancement In Cloud Computing using Deep Learning Techniques

Bal et al [1] presented resource allocation security with efficient task scheduling in cloud computing using a hybrid machine learning RATS-HM technique to address the issues provided by different client needs and rapid data

increase by integrating cloud computing job scheduling and resource allocation. It schedules tasks, minimizes make-span time, and maximizes throughput using an enhanced version of the cat swarm optimization algorithm. In addition, a deep neural network based on group optimization optimizes the distribution of resources while taking resource load and bandwidth limitations into account. By encrypting data, the lightweight authentication technique NSUPREME improves cloud security as a whole. The simulation findings show better performance than current methods in terms of response time, energy usage, and resource utilization. RATS-HM offers a viable option for effective and safe cloud administration, notwithstanding some complications and resource overheads.

Karar et al [2] developed a Faster Region-based Convolutional Neural Network (R-CNN) method that presents a mobile application for automatic pest categorization in agriculture. Crop pest images were taken, processed, and then classified and recommendations were created using a connected pesticide database. Efficiency, accuracy, cost-effectiveness, accessibility, and real-time updates were among the benefits. However, difficulties including reliance on technology, difficulty in setup, privacy issues with data, scope constraints, and upkeep needs occur.

2.2 Review on Security Enhancement in Cloud Computing using Optimization Technique

Kumar et al [3] developed Artificial Bee Colony Optimisation, Particle Swarm Optimisation, and Cuckoo Search Algorithm. The goal of this method was to improve healthcare services by optimizing virtual machines (VMs) in cloud environments. Healthcare data was first gathered from multiple sources and then sent to the cloud via IoT devices. A cloud broker then generates and handles requests from stakeholders. To fine-tune VM allocation, three optimization techniques were used: Evaluation criteria for healthcare procedures include CPU utilization, execution time, stakeholder requirements, and patient data storage. The success of these optimization strategies was evaluated using

experimental analysis and simulations, demonstrating instantaneous increases in system efficiency and execution time. Notwithstanding the potential benefits in terms of improving healthcare services and lowering costs, successful adoption requires addressing issues with complexity, resource intensity, data security, and integration.

Shu et al [4] presented a strong agile response task scheduling optimization method that had been presented to improve cloud computing systems' throughput and resource utilization. Resource load balancing and energy consumption were optimized by the algorithm through dynamic analysis of task arrivals and node heterogeneity. By applying peak energy consumption analysis and agile response techniques, it effectively schedules tasks while reducing task scheduling errors and network congestion. The approach shows enhanced work scheduling efficiency and system stability through experimental assessment. However, because of its complexity, resource overhead, and scalability issues, implementing difficult, requiring considerable thought before deployment.

2.3 Review on Security Enhancement in Cloud Computing using Authentication Framework Technique

Haseeb et al [5] presented the Secure Sensor Cloud Architecture (SASC), to tackle the difficulties in connecting Wireless Sensor Networks (WSN) and the IoT, which offers a creative solution. To improve system intelligence, SASC employs weighted-based centroid vectors and unsupervised machine learning algorithms to intelligently group network nodes. Assuring limitless storage and reliable service delivery for IoT applications, SASC deploys a sensor-cloud infrastructure. As a defence against malevolent network attacks, data security was given top priority by utilising a mathematically infallible one-time pad (OTP) encryption technique. In important parameters including network lifetime, packet drop ratio, energy usage, and transmission overhead, SASC performs better than other state-of-the-art methods, according to simulation trials carried out with Network Simulator. Although it provides improved performance and

scalability, there were obstacles due to the resource requirements and implementation complexity, which call for knowledge and sufficient processing power. However, SASC was a viable option for pushing IoT networks towards security and efficiency thanks to its centralized data management capabilities and strong security safeguards.

Kumar et al [6] offered a technique for secure communication in Vehicular Cloud Computing (VCC) that combines Elliptic Curve Cryptography (ECC) with Radio Frequency Identification (RFID) technology. This framework ensures authentication and anonymity preservation in VCC communication. Authentication requests were encrypted using ECC, and verification was performed by decrypting credentials and validating against stored information. Advantages include enhanced security, anonymity preservation, and resistance against attacks, as validated through formal security analysis and simulation tools. However, implementation complexity and resource overhead were potential disadvantages, along with dependencies on infrastructure and scalability challenges.

2.4 Review on Security Enhancement in Cloud Computing using Data Sharing Technique

Ge et al [7] suggested a Ciphertext-Policy Attribute-Based Mechanism with Keyword Search and Data Sharing(CPAB-KSDS) which tackles the difficulties of safely looking up and exchanging encrypted cloud data. Data confidentiality and access control were guaranteed by CPAB-KSDS through a process flow that includes encryption, attribute-based keyword search, data retrieval, and attribute-based data sharing. Benefits include improved protection against targeted ciphertext and targeted keyword assaults, fine-grained control over data access, effective keyword search, and adaptability in keyword revisions while sharing. However, there were drawbacks due to its difficult installation, difficult key management, and reliance on security presumptions.

Notwithstanding these limitations, CPAB-KSDS exhibits pragmatism and efficacy, rendering it a propitious resolution for safe cloud data administration.

Chadwick et al [8] presented a five-level trust model for sharing sensitive Cyber Threat Information (CTI) amongst cooperating entities was presented by the suggested framework, a cloud-edge architecture, businesses choose the data sanitization technique and trust level want to use before sharing CTI for analysis, providing flexibility and improved security. This strategy addresses worries about the exposure of sensitive information in cyber-security initiatives while promoting cooperation. Potential obstacles were highlighted by implementation complexity, resource needs for certain sanitization techniques, and the requirement for precise trust level selection. Notwithstanding these challenges, the framework has the potential to enhance cyber-security results by facilitating improved CTI availability and fostering stakeholder collaboration.

2.5 Review on Security Enhancement in Cloud Computing using Encryption Technique

Shukla et al [9] suggested the new encryption-based algorithm strengthens data security in this quickly developing field by introducing state-of-the-art methods designed specifically for cloud computing environments. It demonstrates an impressive improvement in many performance indicators over conventional encryption techniques like DES, AES, and Blowfish, thorough study and experimentation. It raises the bar for encryption robustness by improving data secrecy and causing a substantial avalanche effect on plaintext. It was a strong option for protecting sensitive data in cloud-based systems because of its better security features, even with some implementation challenges and resource requirements. This algorithm, with its flexible customization possibilities and compatibility across many cloud platforms, was well-positioned to tackle the changing security concerns of contemporary cloud computing environments.

Orobosade et al [10] presented the AES to strengthen cloud data security, a hybrid encryption technique that combines Elliptic Curve Cryptography (ECC) and AES. Before user data was stored, AES encrypts it to ensure secrecy. For further protection, ECC encrypts the AES key. In cloud environments, this dual-layer strategy improves protection against malevolent intent. Notwithstanding its intricacy and possible impact on performance, the method provides strong data security appropriate for the growing cloud environment. Effective key management was necessary to reduce the complexity that comes with using several different encryption techniques. Overall, by offering a complete security solution, this strategy tackles the increasing vulnerability of sensitive data on the cloud.

3. OBJECTIVES

To enhance security in Data storage and Data Sharing in a cloud computing environment.

To check the user authentication and avoid attackers from theft data in cloud computing, an optimal user authentication protocol is designed.

- Mayfly Optimization with Chaos Based Image Encryption Technique for Cloud Computing Environment.
- Artificial Butterfly Optimization Based Quantum Key Image Encryption Approach for Cloud Security.
- Enhance Security with Improved Honey Badger Algorithm and Anomaly Detection.
- Security Improvement of Cloud Computing by Using Hybrid Cryptography Algorithms.

4. RESEARCH PROBLEM

The research problem addresses the growing challenges of ensuring secure data storage, sharing, and user authentication in cloud computing environments. Traditional cryptographic techniques, such as ECC and RSA, face limitations in balancing security with computational efficiency, especially as the volume of sensitive data increases. To mitigate these challenges, this research

proposes a hybrid cryptographic solution that combines chaotic maps with optimization algorithms like Jellyfish, May Fly, and Artificial Butterfly, Improved Honey Badger Algorithm (HBA) and Anomaly Detection for quantum key image encryption. Additionally, an optimal user authentication protocol is designed to prevent data theft and enhance security. The study aims to implement and validate this approach, comparing its performance against existing methods to determine its effectiveness in improving encryption and authentication processes.

5. ORGANIZATION OF THESIS

Chapter 1: Introduction

This Chapter provides a cloud computing security challenges and the need for advanced solutions to protect data in these environments. It outlines the significance of safeguarding sensitive information and ensuring compliance with regulations such as GDPR and HIPAA. The chapter introduces the concept of shared responsibility between cloud service providers and users, emphasizing the importance of encryption, access control, and monitoring to mitigate security risks. Additionally, it discusses emerging threats, such as data breaches and DDoS attacks, and highlights the necessity of developing optimized user authentication mechanisms and secure transmission methods. It also introduces innovative approaches like the Jellyfish Optimization Algorithm for secure data storage, the MFO-CBIE method for image encryption, Improved Honey Badger Algorithm (HBA)and the ABOA-QKIE technique, which combines artificial butterfly optimization with quantum key encryption to enhance cloud security.

Chapter 2: Literature Review

This chapter provides an overview of the technologies' numerical methods, for enhancing security in cloud computing. This method provides significance, but there are many drawbacks to enhancing security in cloud computing. In this section, the advantages and disadvantages of existing methods

for enhancing security in cloud computing are discussed. The objectives of this research work are also presented.

Chapter 3: Mayfly Optimization with Chaos-Based Image Encryption Technique for Cloud Computing Environment

This chapter introduces a novel Mayfly Optimization with Chaos-Based Image Encryption (MFO-CBIE) method tailored for cloud computing environments. The MFO-CBIE model involves three key steps: image encryption, optimal key generation, and image decryption. The Chaos-Based Image Encryption (CBIE) technique is employed for encryption, while the Mayfly Optimization (MFO) method is used for optimal key generation. Encrypted images are securely transmitted to cloud servers, and decryption occurs upon retrieval. The effectiveness of the MFO-CBIE model is validated through experimental testing with benchmark images.

Chapter 4: Artificial Butterfly Optimization-Based Quantum Key Image Encryption Approach for Cloud Security

This chapter introduces the Artificial Butterfly Optimization Algorithm-Based Quantum Key Image Encryption (ABOA-QKIE) method, which enhances cloud security by encrypting images with a quantum key encryption technique. The ABOA algorithm optimizes key generation for this encryption process. Encrypted images are sent to the cloud server, and quantum key decryption is used to retrieve the original images at the receiving end. The chapter provides experimental validation of the ABOA-QKIE method using various performance metrics on a set of test images.

Chapter 5: Security Improvement of Cloud Computing using Hybrid cryptography Algorithms

This chapter focuses on developing a jellyfish optimization algorithm for secure cloud data storage, implementing it in MATLAB, and evaluating its

performance through encryption and decryption times, comparing it with RSA and ECC-based cryptography methods.

Chapter 6: Enhance Security with Improved Honey Badger Algorithm and Anomaly Detection.

This chapter introduces the Improved Honey Badger Algorithm (IHBA) and advanced anomaly detection techniques to enhance cloud security. Multi-Factor Authentication (MFA) is implemented, combining OTP and biometric verification for robust user authentication. The IHBA-optimized RSA encryption ensures secure data storage and retrieval through advanced encryption and decryption techniques. Density Estimation LSTM s used to capture dynamic cloud behaviour, while the Fractional Stochastic Krill Herd Algorithm (FSKHA) enhances anomaly detection with precise identification of unusual patterns. The chapter validates these methods through experimental analysis using various performance metrics.

Chapter 7: Results and Discussion

This chapter includes an explanation of the results of the three proposed models in addition to a full review of the findings. It gives a brief overview of the conclusions drawn from the examination of the three suggested models. Along with a comparison study, to show the usefulness of the suggested models.

7.1 Performance Analysis of Proposed Models with Previous Models

This section provides a detailed explanation of the proposed approach's performance. To improve security in cloud computing in terms of error analysis, PSNR, and encryption time.

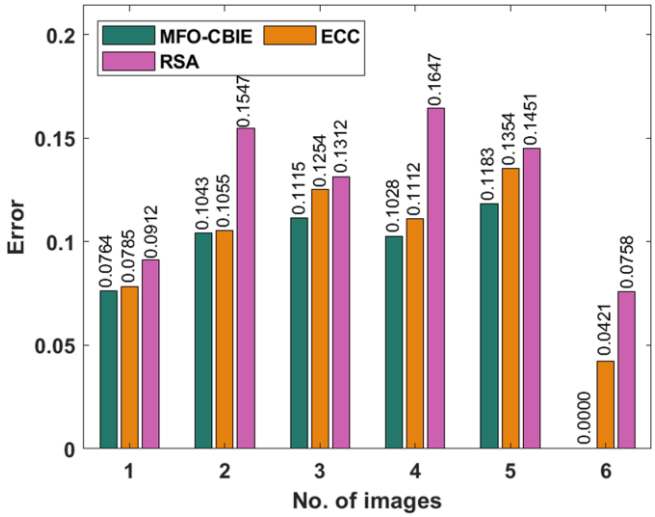

Figure.7.1 Error analysis of MFO-CBIE technique under various test images

Figure 7.1 presents a comprehensive error analysis of the MFO-CBIE method compared to current algorithms. Demonstrating superior performance, MFO-CBIE exhibited the lowest error values across all images, with notably smaller errors compared to RSA and ECC techniques; for instance, achieving an error of 0.0764 in image 1, 0.1043 for image 2, 0.1115 in image 3, 0.1082 for image 4, 0.1183 in image 5 contrasting with higher errors observed in RSA and ECC models.

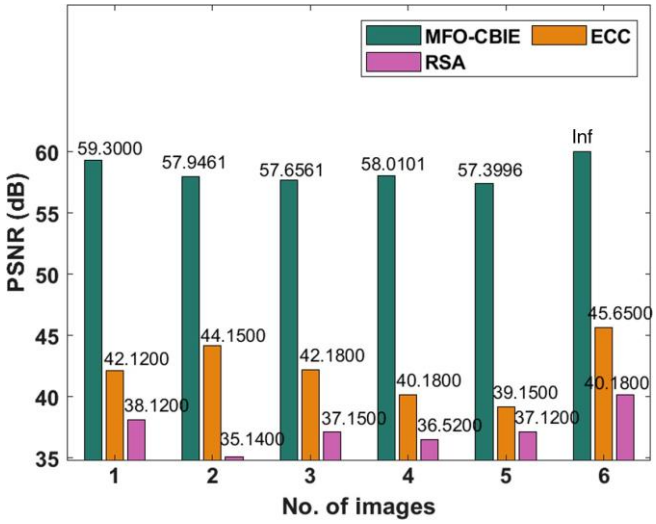

Figure 7.2 Analysis of PSNR

Figure 7.2 represents the higher PSNR of 59.3 dB with image 1, while the ECC and RSA models obtained lower PSNRs of 42.12 and 38.12 dB, respectively. In contrast to the ECC and RSA approaches, which obtained PSNRs of 42.18 and 37.15 dB, respectively, with image 3, the MFO-CBIE approach achieved a superior PSNR of 57.6561 dB. According to picture 5, the MFO-CBIE algorithm has obtained a higher PSNR of 57.3996 dB, while the RSA and ECC systems have only obtained a lower PSNR of 37.12 dB and 39.15 dB, respectively.

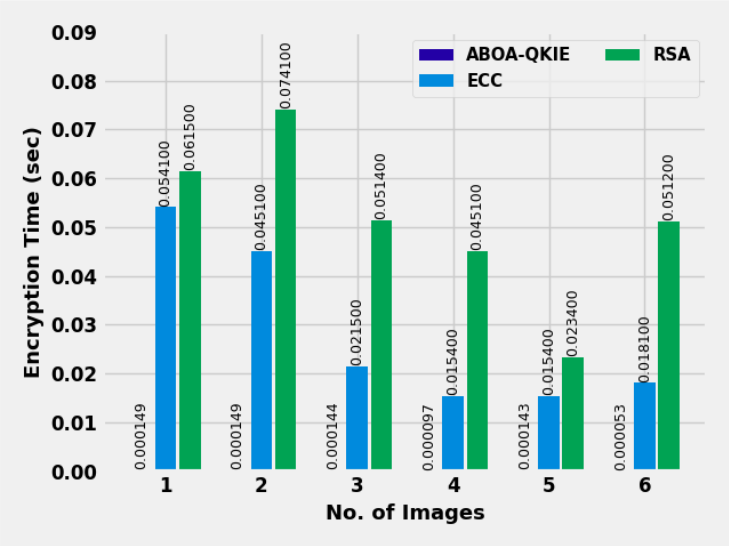

Figure 7.3 ET analysis of the ABOA-QKIE approach under distinct images

In Figure 7.3, the ABOA-QKIE model demonstrated superior efficiency with low ET values across different images. For instance, in image 1, the ABOA-QKIE model achieved an ET of 0.000149s, compared to RSA and ECC models with higher ETs of 0.0615s and 0.0541s, respectively. Similarly, in image 3, the ABOA-QKIE system recorded the lowest ET of 0.000144s, contrasting with RSA and ECC models showing increasing ETs of 0.0514s and 0.0215s. Conversely, in image 6, the ABOA-QKIE algorithm attained the lowest ET of 0.000053s, while ECC and RSA approaches recorded the best ETs of 0.0181s and 0.0512s, respectively.

7.4.1 Comparison analysis of proposed models with previous models

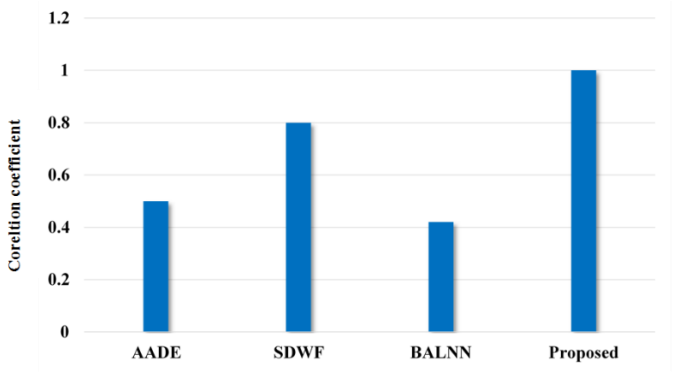

Figure 7.4 Comparison of correlation coefficient of the proposed model

Figure 7.4 represents the correlation coefficient of the proposed model with existing methods. The AADE, SDWF, and BALNN [194] indicate correlation coefficient values of 0.48, 0.8, and 0.41 respectively, whereas the proposed method yields a higher correlation coefficient value of 1 in comparison to existing techniques. This cloud computing metric is a statistical measure that evaluates the correlation between variables. It provides a quantifiable indicator of how changes in one variable impact changes in another, which helps with decisions about resource allocation and optimisation.

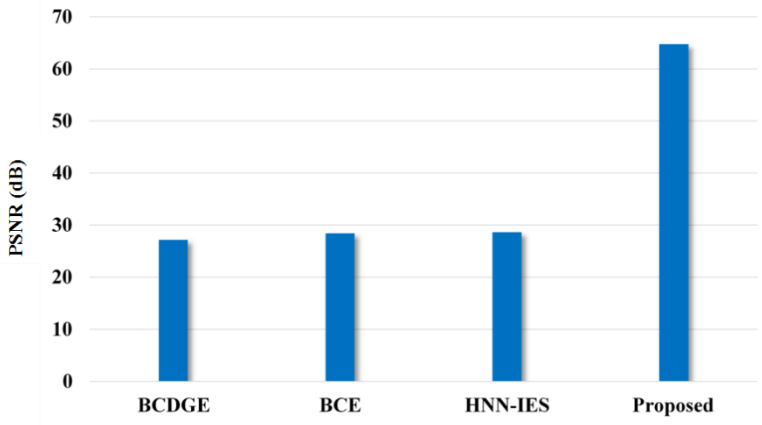

Figure 7.5 Comparison of PSNR of the proposed model

Figure 7.5 illustrates the PSNR comparison between the proposed model and existing methods. While BCDGE, BCE, and HNN-IES achieved PSNR [195] values of 27.17dB, 28.45dB, and 28.62dB respectively, the proposed approach outperforms with a PSNR value of 64.78dB. In cloud computing, PSNR stands for peak picture or video quality as measured quantitatively; it facilitates effective resource allocation and optimizes data transfer for a better user experience.

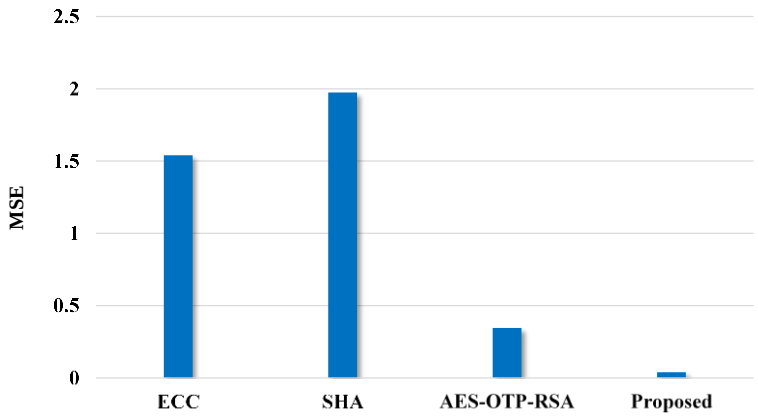

Figure 7.6 Comparison of MSE of the proposed model

The MSE of the suggested model using the existing techniques is shown in Figure 7.6. The suggested method produces a lower MSE value of 0.0383 compared to existing techniques, whereas the ECC, SHA, and AES-OTP-RSA [196] show MSE values of 2.543, 1.975, and 0.345, respectively. The proposed method has the potential to increase predictive accuracy in cloud computing environments, as seen by its much reduced mean square error (MSE) value when compared to alternatives like AES-OTP-RSA, SHA, and ECC. The comparative table for the suggested models is shown in Table 6.1.

Table 7.7 Comparative table for proposed models with existing models

Correlation coefficient			
AADE	**SDWF**	**BALNN**	**Proposed**
0.48	0.8	0.41	1
PSNR (dB)			
BCDGE	**BCE**	**HNN-IES**	**Proposed**
27.17	28.45	28.62	64.78
MSE			
ECC	**SHA**	**AES-OTP-RSA**	**Proposed**
2.543	1.975	0.345	0.0383

7.8 Discussion

Improving resource allocation efficiency, data transfer quality, and forecasting accuracy are the goals of the suggested approach in cloud computing environments. Improvements over current techniques are made in the correlation coefficient, MSE, and PSNR. The comparison analysis shows that the suggested approach performs noticeably better across several important cloud computing-related key metrics. First off, the suggested model scores a perfect 1 for the correlation coefficient, showing a very strong association between the variables. In comparison, the correlation coefficients of AADE, SDWF, and BALNN are 0.48, 0.8, and 0.41, respectively, which are lower than those of other approaches currently in use. The suggested model's better correlation coefficient indicates improved prediction capabilities, which are essential for making well-informed decisions about resource allocation and optimization. With a PSNR value of 64.78 dB, the suggested model performs substantially better than its predecessors, outperforming approaches like BCDGE, BCE, and HNN-IES, which have values ranging from 27.17 dB to 28.62 dB. Significantly higher PSNRs indicate better signal quality and data transmission efficiency, which are

necessary for cloud computing settings to maximize user experience and resource utilization.

Comparing the suggested model's MSE evaluation to those of other methods such as ECC, SHA, and AES-OTP-RSA, which show MSE values ranging from 0.345 to 2.543, reveals a significantly lower MSE value of 0.0383. More predictive accuracy and dependability are indicated by this decrease in MSE, which makes it possible to foresee system behavior and resource needs more accurately. As such, the suggested paradigm has the potential to improve system performance as a whole as well as user happiness in cloud computing environments. Overall, the numerical results demonstrate the significant improvements in correlation coefficient, PSNR, and MSE that the suggested model offers over current techniques. These enhancements highlight how the suggested model has the ability to completely transform cloud computing systems' resource allocation, data transmission quality, and predictive accuracy which ultimately increase user experience and operational efficiency.

Chapter 8: Conclusions and Future Scope

8.1 Conclusions

The goal of this research is to enhance security in cloud computing. This research presents advanced methods to enhance cloud computing security by combining hybrid cryptography, anomaly detection, and optimal key generation. The proposed approaches, such as MFO-CBIE and ABOA-QKIE, ensure secure encryption, efficient key generation, and reliable decryption of data, providing robust protection for cloud storage systems. Techniques like the Jellyfish method and the Improved Honey Badger Algorithm, paired with anomaly detection inspired by krill swarm behavior, enhance threat detection and response capabilities. Experimental evaluations confirm the superior performance of these models, achieving high accuracy, low false alarms, and scalability for dynamic cloud environments. Future advancements in image steganography and related technologies are expected to further elevate cloud security standards.

8.2 Future scope

- The creation of more workable and effective homomorphic encryption techniques allow computation on encrypted material without disclosing private information. This enhances the security of data processing in the cloud.

- Placing Zero Trust Architecture (ZTA) into practice where all access requests are validated and authenticated and no entity is trusted by default greatly improve cloud security. Upcoming improvements entail improving ZTA models and smoothly integrating into cloud infrastructures.

- Cloud computing security improved by integrating blockchain technology, which offers a decentralized, tamper-proof ledger for storing private data like transactions, identity management information, and access logs.

- More sophisticated multi-factor authentication systems, including biometric authentication paired with behavioural analysis, developed to improve access restrictions and stop illegal access to cloud resources.

- Cloud deployments made to comply with industry standards and regulatory regulations by automating regulatory compliance processes in cloud settings with tools and technologies like Compliance as Code (CaC). This improves overall security posture.

- The dangers of supply chain assaults targeting cloud infrastructure reduced by fortifying security protocols throughout the whole supply chain, from cloud service providers to hardware manufacturers.

REFERENCES

[1] P.K. Bal, S.K. Mohapatra, T.K. Das, K. Srinivasan, and Y.C. Hu. A joint resource allocation, security with efficient task scheduling in cloud computing using hybrid machine learning techniques. *Sensors*, **22** (3) (2022), 1242.

[2] M.E. Karar, F. Alsunaydi, S. Albusaymi and S. Alotaibi. A new mobile application of agricultural pests recognition using deep learning in cloud computing system. *Alexandria Engineering Journal*, **60** (5) (2021), 4423-4432.

[3] P. Kumar and K. Silambarasan. Enhancing the performance of healthcare service in IoT and cloud using optimized techniques. *IETE Journal of Research*, **68** (2), (2022),1475-1484.

[4] W. Shu, K. Cai, and N.N. Xiong. Research on strong agile response task scheduling optimization enhancement with optimal resource usage in green cloud computing. *Future Generation Computer Systems*, **124** (2021), 12-20.

[5] K. Haseeb, A. Almogren, I. Ud Din, N. Islam and A. Altameem. SASC: Secure and authentication-based sensor cloud architecture for intelligent Internet of Things. Sensors, **20** (9) (2020), 2468.

[6] V. Kumar, M. Ahmad, D. Mishra, S. Kumari and M.K. Khan. RSEAP: RFID based secure and efficient authentication protocol for vehicular cloud computing. *Vehicular Communications*, **22** (2020),100213.

[7] C. Ge, W. Susilo, Z. Liu, J. Xia, P. Szalachowski and L. Fang. Secure keyword search and data sharing mechanism for cloud computing. *IEEE Transactions on Dependable and Secure Computing*, **18** (6) (2020), 2787-2800.

[8] D.W. Chadwick, W. Fan, G. Costantino, R. De Lemos, F. Di Cerbo, I. Herwono, M. Manea, P. Mori, A. Sajjad and X.S. Wang. A cloud-edge based data security architecture for sharing and analysing cyber threat information. *Future generation computer systems,* **102** (2020),710-722.

[9] D.K. Shukla, V.K. Dwivedi and M.C. Trivedi. Encryption algorithm in cloud computing. *Materials Today: Proceedings*, **37** (2021),1869-1875.

[10] A. Orobosade, T.A. Favour-Bethy, A.B. Kayode and A.J. Gabriel. Cloud application security using hybrid encryption. *Communications on Applied Electronics*, **7** (33) (2020),25-31.

LIST OF PUBLICATIONS

[1] S. Justin and S.K. Karuppusamy. Mayfly optimization with chaos-based image encryption technique for cloud computing environment. *Journal of Electronic Imaging,* **32** (5) (2023),052303-052303.

[2] S. Sheela and N. SubbuLakshmi. Enhancing cloud security with improved Honey Badger Algorithm For Efficient Data Storage and Robust Image encryption. *Journal of Environmental Protection and Ecology* **25** (6) (2024),1803–1812.

[3] S. Sheela and N. SubbuLakshmi. Artificial Butterfly Optimization Based Quantum Key Image Encryption Approach for Cloud Security. *Journal of Computational Analysis and Applications* 33 (6) (2024), 63–77.

[4] S. Sheela and N. SubbuLakshmi. Anomaly Detection in Dynamic Cloud Environment Using Density Estimated LSTM and Stochastic Krill Herd. *Journal of Information Science and Engineering* **38** (0.75) 1016-2364.

[5] S. Sheela and N. SubbuLakshmi. Security Improvement of Cloud Computing by Using Hybrid Cryptography Algorithms. SN Computer Science, Springer Nature, 2661-8907.